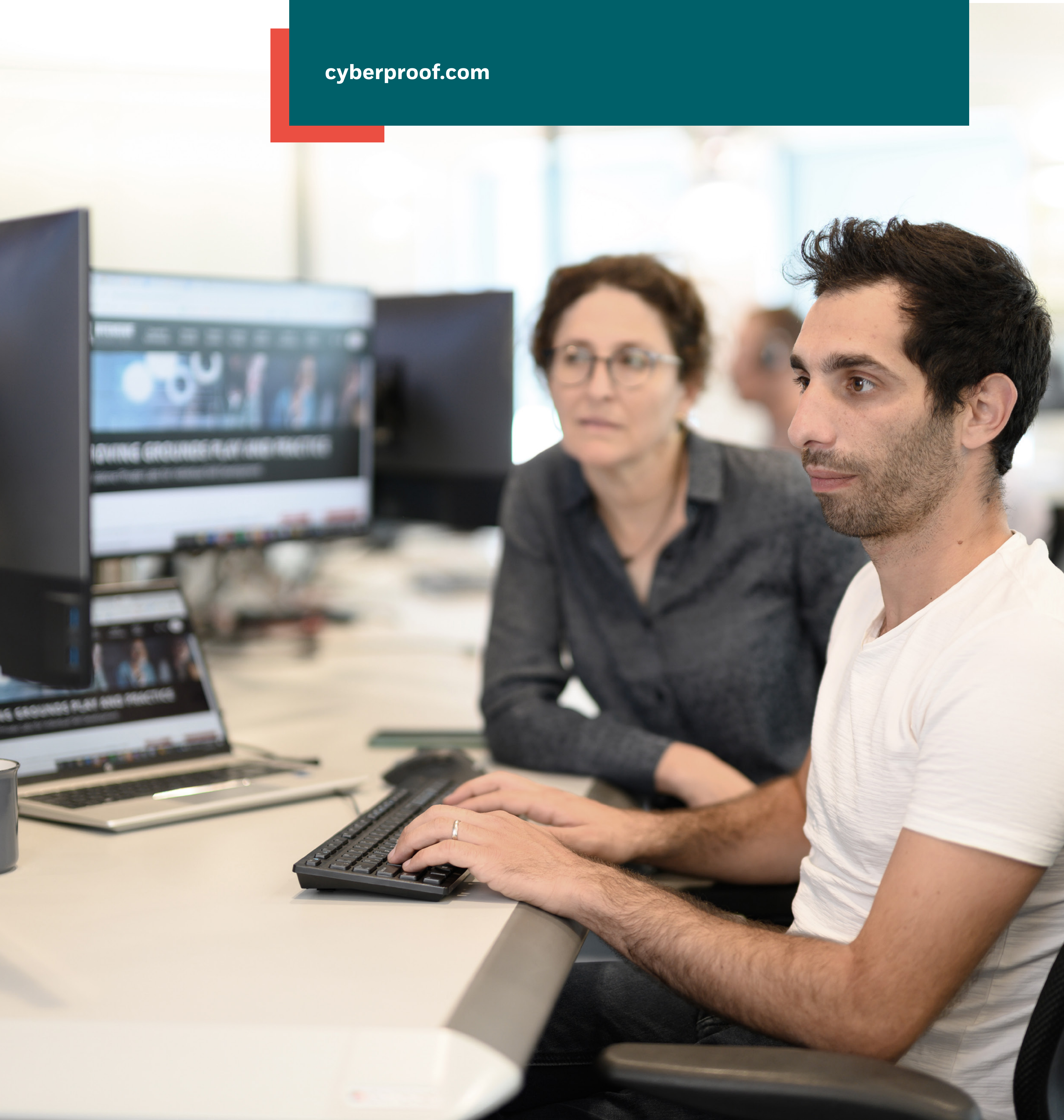
CyberProof®
A UST Company

Managed XDR for Google Cloud

cyberproof.com



Using a unique combination of security engineering and operational capabilities, CyberProof helps you stay secure as you modernize your infrastructure from legacy and on-prem to cloud-native cybersecurity defenses. Our enterprise-scale approach allows us to effectively anticipate, adapt, and respond to cyber threats while providing you with unmatched adaptability, transparency, and control.

How CyberProof can help

Platform-led delivery with the CDC

The CyberProof Defense Center (CDC) platform acts as a single pane of glass for security operations, integrating with both legacy SIEMs and Google Chronicle, so you can take a phased approach to cloud migration while maintaining visibility of both on-premises and cloud security alerts and incidents.

Enhanced visibility with custom use cases

CyberProof provides consulting, engineering and operational expertise to transform your cyber defense operation. Our DevOps deployment model provides rapid time to value by establishing customized Google Chronicle infrastructures and use case content.

Managed Extended Detection & Response services

Our global Security Operations teams is a force multiplier, carrying out day-to-day security operations from alert monitoring, triage and validation to threat intelligence, threat hunting, and incident response. The CDC platform is a service delivery platform, coordinating multiple teams and processes that include SLAs and KPIs for continual service improvement.

KEY FEATURES

- A team of cyber experts around the globe conducts detection and response services across your entire IT environment
- Our CyberProof Defense Center (CDC) platform natively integrates with Google . Leveraging Chronicle SIEM, we provide a single interface for accelerated detection & response activities
- Setup and configuration of Google Chronicle SOAR, SIEM, and cloud security tools
- Advanced security engineering, to support non-standard data sources, complex log management, regulatory compliance, cost optimization, and advanced analytics

Optimizing your cyber defense

24/7 SOC monitoring - Cyber threats can arise at any time, and a delay in detection and response can be costly. Continuous monitoring ensures that threats are identified and addressed promptly. CyberProof's dedicated SOC team monitors security alerts and incidents 24/7 and is equipped to respond to alerts in real-time, escalating as necessary

Integrate logs from any source – We can connect all data types from any source. This improves the flow and handling of data, augmenting Google Chronicle's rules and capabilities to provide clients with automated and dynamic threat detection.

Advanced threat detection & response – Without effective detection, an organization remains vulnerable to sophisticated attacks that bypass traditional security measures. CyberProof offers robust threat detection mechanisms using behavioral analytics, machine learning, and AI-driven algorithms - offering rapid response to isolate compromised systems, mitigate threats, and minimize the potential impact of attacks.

Continuous Improvement – CyberProof's Use Case Factory is an agile development methodology led by use case engineers and developers. It continuously identifies and fills detection and response gaps with customized use case content. Our Use Case Catalog consists of detection rules, digital playbooks and third-party API integrations for response automation.

Automated investigation and analysis - Swift and accurate incident investigation is crucial to understanding the scope and nature of a breach. Effective analysis allows for targeted response and future prevention efforts. CyberProof leverages automated incident investigation tools that reconstruct attack timelines, provide visual representations of attack chains, and offer insights into the tactics, techniques, and procedures used by adversaries.

Transitioning you to cloud-native cyber defense

We provide a combination of consulting, engineering and managed security expertise to transform you to cloud-native security operations leveraging Microsoft Sentinel and Defender Suite.

Plan

- Understand your business goals, security objectives and the maturity of your current SOC process
- Design a plan to migrate to Google Chronicle infrastructure and Google Chronicle solutions

→

Transition

- Knowledge gathering and service operations takeover, with resource mobilization
- Stabilize existing services, and improve processes
- Plan phased decommission of legacy security analytics solution
- Deploy a scalable, cloud-native, security infrastructure

→

Transform

- Establish Cloud-Native Monitoring Infrastructure and required Google Chronicle solutions
- Connect to CDC platform for centralized, transparent security operations
- Configure custom use cases, detection rules, hunting queries and digital playbooks

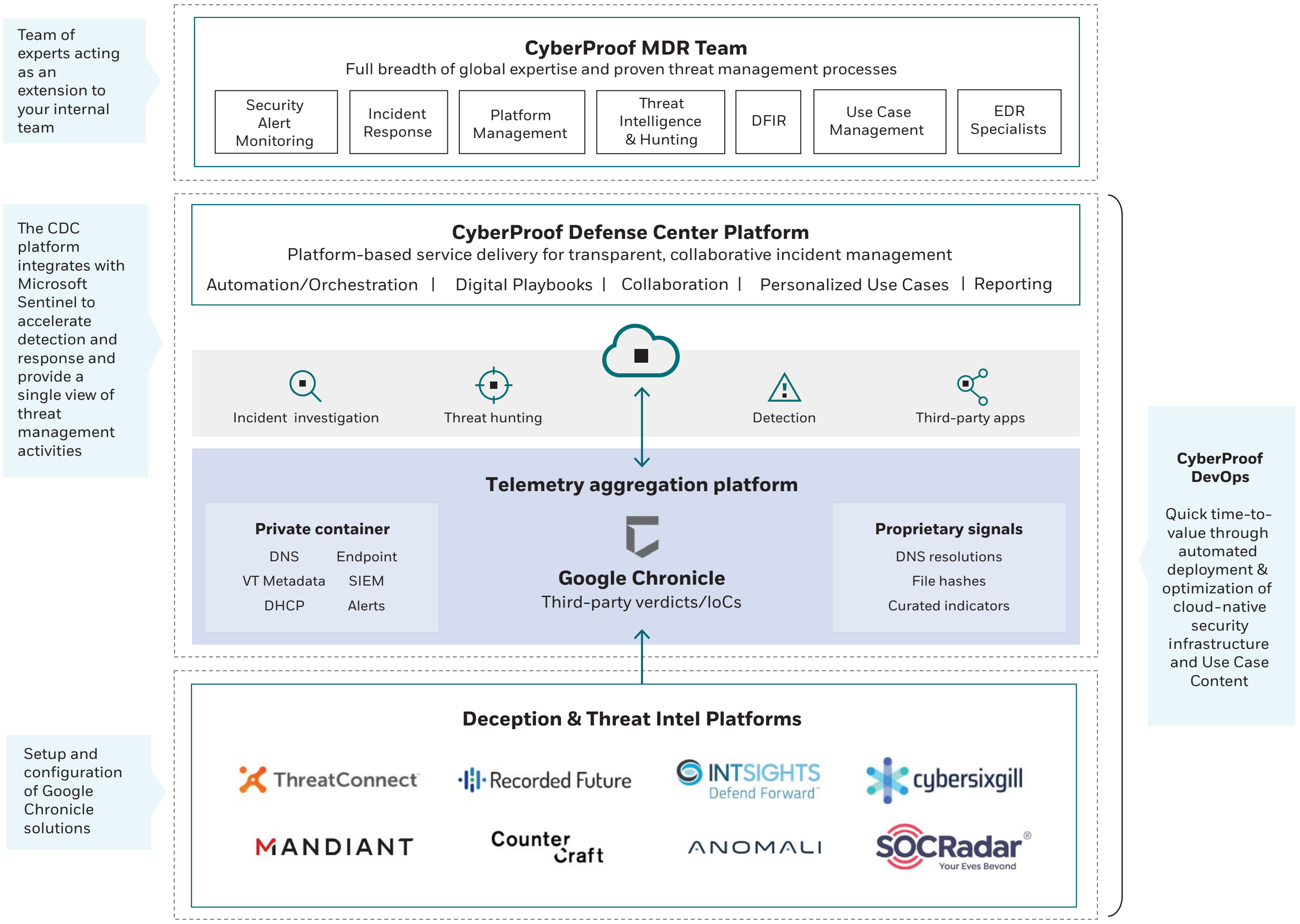
→

Operate

- Provide continuous Security Event Monitoring, Threat Detection & Response services
- Create customized dashboards and reporting as well as actionable threat intelligence on targeted threats

Next-gen, cloud-native MDR service architecture

Our MDR service architecture leverages the full breadth of expertise provided by our global team, our proven threat management processes, real-time collaboration and escalation procedures, and platform-led technology delivery – allowing us to integrate Google Chronicle's XDR technology into our end-to-end MDR service.



Team of experts acting as an extension to your internal team

CyberProof MDR Team

Full breadth of global expertise and proven threat management processes

Security Alert Monitoring | Incident Response | Platform Management | Threat Intelligence & Hunting | DFIR | Use Case Management | EDR Specialists

The CDC platform integrates with Microsoft Sentinel to accelerate detection and response and provide a single view of threat management activities

CyberProof Defense Center Platform

Platform-based service delivery for transparent, collaborative incident management

Automation/Orchestration | Digital Playbooks | Collaboration | Personalized Use Cases | Reporting

Incident investigation

Threat hunting

Detection

Third-party apps

Telemetry aggregation platform

Private container

DNS, Endpoint, VT Metadata, SIEM, DHCP, Alerts

Google Chronicle

Third-party verdicts/IoCs

Proprietary signals

DNS resolutions

File hashes

Curated indicators

CyberProof DevOps

Quick time-to-value through automated deployment & optimization of cloud-native security infrastructure and Use Case Content

Setup and configuration of Google Chronicle solutions

Deception & Threat Intel Platforms

CyberProof®
A UST Company

About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts.

Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics.

Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations.

For more information, visit www.cyberproof.com

Locations
Barcelona | California | London | Paris | Singapore | Tel Aviv | Trivandrum